



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

#26
209,1099
S. Sand
1/16/03

RECEIVED

JAN 16 2003

Technology Center 2100

Appellants: Howard Udell et al.

Serial Number: 09/098,204

Filed: June 16, 1998

Entitled: **SELF-DESTRUCTING DOCUMENT AND
E-MAIL MESSAGING SYSTEM**

Examiner: Thong Vu (Art Unit 2756)

BOX: APPEAL

Assistant Commissioner for Patents
Washington, DC 20231

January 6, 2003

APPELLANTS' REPLY BRIEF UNDER 37 C.F.R. § 1.193

S I R:

Appellants submit this Reply Brief Under 37 C.F.R. § 1.193 to the Examiner's Answer dated November 5, 2002 for the consideration of the Board of Patent Appeals and Interferences in support of Appellants' appeal of the final Office Action dated October 31, 2001 in the above-identified application. As discussed below, Appellants submit that the comments in the Examiner's Answer are not supported by the cited prior art references. Appellants respectfully request that the rejections be reversed.

I. Rejection of Claims 1-10, 13-15, 17-19 and 44-47 Based Upon Hansen and Beck

A. Group I: Claims 1-4 and 44-47

In response to Appellants' argument that Hansen does not disclose a method for creating a self-destructing document, the Examiner claims that Hansen teaches enhanced documents with embedded scripts that can automatically perform functions such as deleting a file. The Examiner states that Hansen also teaches a hypertext document, such as a Hypercard, that can be created as an enhanced document with embedded object forms with a defined set of trigger events, and one of the document's embedded scripts could trigger a file-delete function. Citing Hansen pages 23-29,

30 and 32, the Examiner argues that it is well known that a delete file function could delete a specific document that was defined by the user or could delete itself.

However, Hypercard is not discussed in Hansen to the extent implied by the Examiner but rather is actually mentioned only at pages 23, 24, 26 and 28 of Hansen, and then only as a possible tool to enable users to avoid viruses embedded in a document. Hansen does not teach or suggest a self-destructing document, as alleged by the Examiner. Below, each of the sections of Hansen that mention Hypercard are reviewed.

Hansen discusses creation of enhanced documents that have various animations and simulations to illustrate the points of the document (page 23, column 1) and relates to solving the security problem that is caused by scripts embedded within these enhanced documents (page 28, column 2). In this context, hypertext documents are mentioned as a way of enabling enhanced documents. According to Hansen, the “best known system with a programming language for enhancing what the reader sees is Hypercard” (page 24, column 1), and, in order to connect each object to the portion of the script that specifies the response to events on that object, Hypercard associates a script with each object (page 24, column 2). Hansen acknowledges that execution of scripts embedded in a document “is a security loophole” that detracts from a document’s security by ceding control to the embedded script (which can delete, modify or send a file). Appellants note that this is the well-known problem of a virus, which executes a program embedded within one file to operate on or be destructive towards other files in the user’s operating system, and a self-destructing document is not taught or suggested in this portion of Hansen.

Hansen also mentions hypertext documents as a way of avoiding the security problem of scripts embedded in enhanced documents: “Hypercard offers a security level scheme of a sort: users may choose to execute at one of five levels of privilege.” Hansen acknowledges that these security levels restrict only the user from taking dangerous operations but do not restrict the script itself, which may still even reset the security level. Hansen then discusses other options of avoiding executing the embedded scripts and their security problems, options such as a text surrounding the Ness script or a dialog box that appears on the user’s monitor (page 28, column 2 – page 29, column 1), both of which alert the user to the presence of the embedded script and

provide the option of not executing the potentially-destructive embedded script. This passage of Hansen also does not teach or suggest a self-destructing document.

Thus, Hansen, in these references to Hypercard or anywhere else in that document, does not support the Examiner's conclusion that "it is well-known in the art that a delete file function could be deleted a specific document which defined by user or itself as claimed" (emphasis added). Whereas Hansen does teach embedding of scripts or viruses that may contain a delete-file function to delete other files within the user's system, Hansen does not teach or make obvious embedded program that deletes the very document to which it is attached. The Examiner has not provided even a suggestion in the art that a delete file function could delete the specific document to which it is attached. The Examiner's allegations of obviousness are not supported by the cited references, as Hansen does not mention or even suggest a method for creating a self-destructing document, wherein the user has no control over the document's destruction of itself, as claimed in claims 1-4 and 44-47.

B. Group II: Claims 6-10, 14-15 and 17

The Examiner misstates Appellants' argument as contending that "the prior art does not teach an e-mail messaging system". The Examiner attempts to counter this argument, first by stating that Hansen teaches an embedded script in a document designed to delete a file or multimedia mail (Hansen pages 23 and 29), and then by summarily concluding that it is obvious to one of ordinary skill in the data processing art that an e-mail message that contains a delete file function could automatically self-destruct (i.e., event trigger) or delete another file by design.

However, Appellants do not contend that the prior art does not teach an e-mail messaging system. Rather, Appellants have pointed out that the prior art, alone or in combination, does not disclose a self-destructing e-mail messaging system. The Examiner has still not demonstrated any disclosure or suggestion anywhere in Hansen or Beck, or elsewhere, of an e-mail message with an attachment that causes the e-mail message to be automatically deleted after a predetermined expiration date or condition is met, as required by claims 6-10, 14-15 and 17.

Also, for the first time, the Examiner alleges that Hansen “teaches an embedded script in a document designed to delete a file such as Hypertext document or multimedia mail”. Yet, Hansen teaches no such thing regarding multi-media mail. At pages 23-24, Hansen states,

Some discussion in the multi-media mail community has focused on using a language to describe mail documents. With this facility, new varieties of objects can be sent if the receiving system has no more capability than the language interpreter. The work reported below ... is not a language suitable for describing any object, it assumes that a collection of objects will be available in the software of both sender and receiver. It does, however, provide a language tailored for the author to describe a myriad of different forms of interconnection and behavior of objects.

And, at page 29, Hansen states,

Although apriori it may seem that enhanced documents would be excellent for mail, they turn out not to be used in mail very much. The world of electronic mail is much more a world of short immediate messages than it is a world of carefully crafted communication. Plans for multi-media mail must satisfy the requirement for transmission of a variety of kinds of bulk information – including scripts – but this will not be the majority of the traffic.

These two sections are the only mention in Hansen of multi-media mail. There is no teaching that a script embedded in an e-mail could delete a file, as alleged by the Examiner. Neither section of Hansen contains any hint of the elements of claims 6 and 17 relating to a self-destructing e-mail messaging system wherein an executable module attached to an e-mail message automatically deletes the very e-mail message to which it is attached based solely upon a preselected expiration date or a predetermined condition such as an attempt to print, copy or forward the message. Furthermore, the Examiner has not even attempted to demonstrate how it is obvious to one of ordinary skill in the data processing art from the disclosures of Hansen to make an e-mail message that could automatically self-destruct. In fact, the lack of such teachings in the cited art illustrates that it is not obvious to create the self-destructing e-mail messaging system as claimed.

The Examiner also misstates Appellants’ argument as contending that “the prior art does not teach deleting a file when a predetermined condition is selected.” The Examiner attempts to counter this argument by stating that Beck discloses an e-mail with an attachment message that may be automatically deleted after a given time limit (i.e., an expiration date), and then by summarily concluding that it is obvious that the predetermined condition to delete the e-mail

message with attachment could be changed by the time limited, the option of e-mail function (i.e., saved by one or several days, weeks or months) as a variable subject matter.

However, Appellants do not contend that the prior art, such as document retention systems, does not teach deleting a file when a predetermined condition is selected. Rather, Appellants have pointed out that Beck does not disclose an e-mail message with an attachment that causes the e-mail message to be automatically deleted after a predetermined expiration date or upon a predetermined condition.

Indeed, in Beck, the e-mail message does not actually have a document or any executable module attached to itself but rather contains only a network address to a document on a remote web server. It is only the document at that network address, not the e-mail itself, that is actually deleted upon a certain condition (see Column 7, lines 1-18). Even the Examiner does not allege that the e-mail message itself, which remains untouched, is deleted. Moreover, in Beck, the document is not deleted by some executable code that is attached to the e-mail or to the document but rather by a document retention program. Thus, there is no disclosure or suggestion in the prior art of an executable module that operates on the very e-mail message to which it is attached, deleting it at a preselected expiration date or upon a predetermined condition.

C. Group III: Claims 5 and 13

The Examiner again misstates Appellants' argument as contending that the prior art does not teach that the executable module executes when the document or e-mail message to which the module attached is opened. The Examiner then contends that the prior art taught a hypertext document (a multimedia e-mail or Hypercard) that, when opened, could trigger an event such as a birthday song or another function, such as deleting a file (Hansen, pages 23-24 and 28-32).

However, Appellants do not argue that the prior art does not teach an executable module that executes when a document to which the module is attached is opened. Instead, Appellants have pointed out that the prior art does not disclose an executable module attached to a document or e-mail message that executes when the document or e-mail message to which it is attached is opened, as required by claims 5 and 13, i.e., to thereby cause the document or e-mail message to which it is attached to be deleted if the predetermined expiration date has passed.

The Examiner's reliance on Hansen's mention of hypertext documents does not support his arguments. In Hansen, the executable module, i.e., the Ness script, is executed when the user chooses to do so, not when the document is opened, as alleged by the Examiner, and not to delete the very document to which it is attached. Hansen's ways of allowing the user to not execute the embedded script, such as by a text surrounding the script or a dialog box on screen, are useful only if the user has already opened the document. By requiring the user to open the document to use the Ness script and dialog box, Hansen precludes the possibility of a user satisfying the methods of claims 5 and 13, which require that the document or e-mail be deleted upon being opened.

Thus, Hansen does not teach or suggest the steps of executing the executable module when the document is opened and thereby deleting the document if the preselected expiration date has passed, as claimed in claim 5. In addition, the Examiner's arguments are silent regarding any teachings in the prior art of the steps of executing the executable module when the e-mail message to which it is attached is opened and thereby deleting the document if the preselected expiration date has passed, as claimed in claim 13.

D. Group IV: Claims 18 and 19

In all rejections of claims 18 and 19 until now, the Examiner had maintained that the element of the executable module instructing the computer to decrypt the document or e-mail message, if not expired, was disclosed in Hansen. In the Appeal Brief, Appellants demonstrated that reference to Hansen was inapplicable since Hansen did not discuss the use of encryption. The Examiner has apparently withdrawn this basis for rejection and does not now rely on Hansen in an attempt to reject these claims. Instead, the Examiner has asserted a new basis of rejection, that Beck (at column 7, lines 19-40) taught an e-mail message with encryption and decryption keys and that it is obvious that the option of using encryption of a document or an e-mail was well known in the art. However, Beck fails to support the Examiner's new argument for rejection.

According to Beck, because the "attachment" file is visible to other users of the network, one method of ensuring that unauthorized users browsing the WWW HTTP server are unable to obtain a usable copy of the "attachment" file is to store the file in encrypted form and to transmit the decryption key with the original e-mail message. Unauthorized users are thereby prevented

from opening the file, and only the intended user is allowed to access the file using the decryption key that was sent within the e-mail message that referenced the file on the server.

However, it is not “encryption of a document or e-mail that is attached to an executable module”, as alleged by the Examiner, that is claimed in claims 18 and 19. Claims 18 and 19 instead require that the executable module attached to an encrypted document or e-mail message automatically instruct the computer to decrypt the document or e-mail message if it is not expired and to delete the document or e-mail message if it is expired. This step is taken automatically by the executable module and is very different from Beck’s system of attaching an encryption key to an e-mail, whereby the user must himself actually check if the document or e-mail message is expired and only then himself decrypt or delete the message. The system of Beck provides no teaching or suggestion of the steps of claims 18 and 19.

E. No Prima Facie Rejection Made Based on Hansen and Beck

The Examiner fails to establish a prima facie case of obviousness. Hansen did not teach multimedia mail having embedded scripts to delete e-mail messages and certainly did not teach deleting the very e-mail messages within which the scripts are embedded. Also, Beck does not relate to an executable module that is attached to an encrypted document or e-mail message and that instructs the computer to decrypt the document or e-mail message if it is not expired and to delete the document or e-mail message if it is expired. In fact, the subject matters of Hansen and Beck are not at all related to each other, and one skilled in the art would have no motivation to combine these references.

In addition, the Examiner’s statement of “motivation” (“to improve the security and protection [of] the email message with embedded script” to “provide more security and reliability for storage and transaction of the electronic messages in network environment”) is unrelated to Appellants’ invention. Thus, because none of the claims is related to improving the security and protection of e-mail messages or to providing security or reliability for storage and transaction of electronic messages in a network environment, even one skilled in the art so motivated would not think to combine Hansen and Beck for that purpose. In addition, were Hansen and Beck combined for the purpose of the claimed invention, adding the encryption feature of Beck to the disclosure of

Hansen would still not solve Hansen's security problem, since the embedded script would then be encrypted but may still have a destructive effect once decrypted. The Examiner has not alleged how or why one would be motivated by Hansen and Beck or by the prior art to create a document or e-mail message having an embedded module that serves to delete the very document or e-mail message to which it is attached, as claimed by Appellants, or even how combining these references makes the claimed invention obvious.

Accordingly, the Examiner has not provided any proper suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine Hansen and Beck with respect to the pending claims.

II. Rejection of Claims 1-10, 13-15, 17-19 and 44-47 Based Upon Drake and Norin

A. Group I: Claims 1-4 and 44-47

In the Examiner's Answer, the Examiner responds to Appellants' argument that the prior art does not disclose a method for creating a self-destructing document by stating that Drake's abstract taught an e-mail message containing a self-executable code, such as a virus, which destroys itself or other documents. However, this allegation regarding Drake is completely unsupported. Drake discusses security measures for preventing attacks on executable software and, in this context, common viruses and other attacks on such software. The abstract refers to a "software-based computer security enhancing process and graphical software-authenticity method, and a method to apply aspects of the two", which "provides protection against certain attacks on executable software by persons or other software used on the computer." According to the Drake abstract, "[s]oftware using this process is protected against eavesdropping (...), local and remote tampering (...), examination (...), tracing (...), and spoofing (...) by rogues (...)" by means such as "executable encryption, obfuscation, anti-tracing, anti-tamper & self-verification, runtime self-monitoring, and audiovisual authentication".

Nowhere in the Drake abstract or even in the Drake specification is there any mention or suggestion of a self-executable code, such as a virus, which destroys itself, as alleged by the Examiner. In fact, nowhere in the entire text of Drake is there any mention or suggestion of a

document or an e-mail message that contains a self-executable code that destroys the document or e-mail message. Thus, the Examiner's comments are completely unsupported.

B. Group II: Claims 6-10, 14-15 and 17

In response to Appellants' arguments that the prior art does not teach an e-mail system "that is configured to create the message, transmit the message and attach the executable module to the message", the Examiner answers that the prior art taught an e-mail system with an expiration date, encryption key, viewing the executable program such as software designed to self-destruct (Drake at column 7, lines 43-52) or viruses (Drake at column 1, line 55 – column 2, line 50) that are embedded or attached to the e-mail message as a well-known feature.

However, the Examiner's citations do not support his contentions as to Drake's teachings. Drake discusses attempts to breach security of computer systems, such as an e-mail virus (columns 1-2) and tracing the execution of software (debugging, at column 7). Drake teaches how to detect when debugging is taking place so as to make the detection and bypass of debug-detection more difficult, and, in this regard, at column 7, lines 43-52, provides a method of hampering debugging by intentionally storing code or critical data in a particular area of memory whose contents are deleted upon an unexpected use of memory. By having the rogue delete the very code or data that he desires to access, the rogue is thereby prevented from accessing that code. Drake also advises that use of strong encryption will also hamper the disabling of such prevention routines.

Whereas Drake mentions destructive e-mail viruses, nowhere does Drake discuss the use of an e-mail messaging system to accomplish self-deletion of the e-mail message. Contrary to the Examiner's assertions, Drake does not teach self-deletion by an e-mail message or a document, and Drake certainly does not teach deletion of a document by an executable module attached to that document. The deletion in Drake performed not by an executable module that is attached to the data or code but rather by tracing software, an external program, which is tricked into deleting the very information that it seeks to obtain. Thus, no self-deletion is actually performed. As such, the Examiner's comments are completely unsupported, and Drake in no way discloses or suggests self-deletion by an executable module of the e-mail message to which the module is attached, at a preselected expiration date or condition, as required by claims 6-10, 14-15 and 17.

C. Group III: Claims 5 and 13

In response to Appellants argument that “the prior art does not teach create and activate the self-destructing document”, the Examiner again answers that the prior art taught an e-mail system with software designed to self-destruct (Drake at column 7, lines 43-52) or viruses (Drake at column 1, line 55 – column 2, line 50). According to the Examiner, it is well known in the art that the viruses as an executable code self-activate and destruct documents.

In reply, Appellants note that the Examiner’s citations do not support his contentions. Although it is known that viruses may, in some cases, execute and then damage or delete other files in the user’s system, the text of Drake at columns 1-2 and 7 cited by the Examiner does not teach self-destruction by a document or e-mail, as claimed. Instead, Drake teaches a deletion performed by an external software-tracing program. No self-deletion of a document or e-mail message by an executable module that is attached to the document and is configured to execute when the document or e-mail is opened is disclosed in Drake.

The Examiner has cited no prior art that teaches or suggests an executable module attached to a document or e-mail message that executes when that document or e-mail message is opened, to thereby cause that document or e-mail message to which it is attached to be deleted if the predetermined expiration date has passed. The Examiner’s unsupported and conclusory assertions that it is a “well known” feature cannot substitute for an actual prior art citation of disclosure of these elements.

D. Group IV: Claims 18 and 19

The Examiner asserts that Appellants argue that “the prior art does not teach the e-mail message is encrypted”. The Examiner counters this argument by noting that Drake teaches an e-mail message with encrypted technique (at Figure 11; column 3, lines 45-50; column 4, line 50; column 5, line 63 – column 6, line 3; and column 8, lines 39-53). However, these statements regarding Drake are completely besides the point of Appellants’ invention. Claims 18 and 19 do not claim encryption of a document or e-mail message. Instead, claims 18 and 19 require that the executable module that is attached to an encrypted document or e-mail message automatically instruct the computer to decrypt the document or e-mail message if it is not expired and to delete

the document or e-mail message if it is expired. This alternative step is taken automatically by the executable module and is very different from the disclosures of Drake.

In the portions of Drake cited by the Examiner, Drake describes uses of encryption in order to prevent access to computer software, and Figure 11 shows the execution of the new executable. However, Drake provides no teaching or suggestion of automatic decryption by an executable module of a document or e-mail message to which it is attached if the document or e-mail message is not expired and automatic deletion of the document or e-mail message by the executable module if the document or e-mail message is expired.

E. No Prima Facie Rejection Made Based on Drake and Norin

The Examiner has provided no proper suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine Drake and Norin with respect to the claims. Because the subject matters of Drake and Norin are not related to one another, one skilled in the art would have no motivation to combine these references. Furthermore, were Drake and Norin combined for the purpose of the claimed invention, adding the security-enhanced executable replacement system of Drake to the server communication network for keeping track of changed data of Norin would still not produce the claimed self-destructing document or e-mail messaging system.

Accordingly, the Examiner has failed to establish a prima facie case of obviousness of the claims based upon Drake and Norin.

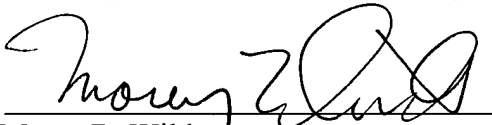
III. CONCLUSION

Appellants' claimed methods and systems are substantially different from anything cited in the prior art references, Hansen, Beck, Drake or Norin, taken alone or in combination. The claimed methods and systems have steps and elements that are not disclosed or even suggested in the cited prior art, and Appellants believe that for the foregoing reasons the final rejections of claims 1-10, 13-15, 17-19 and 44-47 should be reversed.

Prompt consideration of the arguments presented herein and reversal of the final rejections is earnestly solicited.

Respectfully submitted,

DAVIDSON, DAVIDSON & KAPPEL, LLC

By: 
Morey B. Wildes
Reg. No. 36,968

DAVIDSON, DAVIDSON & KAPPEL, LLC
485 Seventh Avenue, 14th Floor
New York, NY 10018
Tel: (212) 736-1940